Algoritmos para resolver el problema de rango mínimo para matrices 3-dimensionales y su aplicación a la seguridad de criptosistemas basados en polinomios cúbicos

Snayder José Buelvas Castellar

Tesis presentada como requisito
para optar por el título de
Master en Matemáticas

Asesor
Daniel Cabarcas Jaramillo

UNIVERSIDAD
NACIONAL
DE COLOMBIA

Escuela de Matemáticas
Facultad de Ciencias
Universidad Nacional de Colombia, Sede Medellín
Agosto, 2019

Índice general

Introducción

En palabras muy sencillas, un criptosistema es un algoritmo o algoritmos usados para permitir la comunicación segura entre usuarios. Los criptosistemas pueden ser clasificados de dos maneras; criptosistemas de llave simétrica, donde los usuarios comparten una llave secreta que es usada tanto para encriptar como desencriptar y criptosistemas de llave pública, donde cada usuario tiene un par de llaves, una llave pública y una privada. Así si un usuario A desea enviar un mensaje a un usuario B, A debe encriptar la información con la llave pública de B y este desencripta usando su llave privada. El criptosistema RSA es un ejemplo de criptosistema de llave pública.

En 1995, Peter Shor [Sho97] propone un algoritmo cuántico para la factorización de números enteros capaz de ejecutarse en tiempo polinomial. Este hecho hizo, en teoría, inseguros algunos criptosistemas, como por ejemplo los basados en factorización de enteros (RSA) y logaritmo discreto (criptografía de curvas elípticas). Debido al auge de investigaciones alrededor de la computación cuántica, la criptografía post-cuántica ha ganado relevancia en los últimos años. En diciembre de 2016, NIST (US National Institute of Standards and Technology) hizo un llamado para estandarizar las propuestas post-cuánticas, entre esas propuestas destacan los criptosistemas de llave pública multivariada (MPKC) [DGS06].

La idea central de los sistemas MPKC es tomar una tupla de polinomios cuadráticos multivariados y utilizarlos para la encripción y desencripción de mensajes. La encripción se realiza evaluando un mensaje m en estos polinomios y la desencripción consiste en invertir la tupla de polinomios. La seguridad recae en el hecho de que invertir un sistema de polinomios multivariados es un problema NP-completo. Sin embargo, estos sistemas pueden tener otro tipo de vulnerabilidades que los hacen inseguros. Los criptosistemas MPKC que se han propuesto como esquemas de encripción se han demostrado inseguros, por otro lado los esquemas de firmas digitales se han probado, hasta ahora, seguros para su implementación. De hecho, en la competencia de NIST aún podemos encontrar en competencia sistemas MPKC en el área de firmas digitales, tales como GeMSS [CFMR$^+$17].

Es bien conocido que una manera de atacar un criptosistema MPKC es resolviendo una instancia del problema del rango mínimo. El problema de rango mínimo es, dado k matrices de $m \times n$ y un número r, determinar cuando existe una combinación lineal de las k matrices que tenga rango menor o igual a r. A pesar que este es un problema NP-completo, existen algoritmos eficientes que lo resuelven para ciertos parámetros. En efecto, Kipnis y Shamir propusieron un ataque al sistema HFE como un problema de rango mínimo [KS99]. Desde entonces se conocen ataques similares para otros sistemas MPKC.

Dado lo anterior, es natural preguntarse si podemos basar un esquema de encripción

MPKC en polinomios cúbicos y si esto representa mayor seguridad para el criptosistema. La motivación para hacer esto radica en el hecho que los polinomios cúbicos pueden ser asociados con matrices tres dimensionales, las cuales pueden llegar a tener un rango mayor a las dos dimensionales. En [Osp16] se introduce un criptosistema llamado HiRaC(High Rank Cryptosystem) basado en polinomios cúbicos. Un análisis previo de HiRaC [EO$^+$] muestra que el polinomio central del criptosistema tiene asociada una matriz cúbica de rango alto que nos permite asegurar que un ataque algebraico directo es ineficiente.

En el presente trabajo analizamos la seguridad de HiRaC con respecto al ataque de rango mínimo. En los capítulos 1 y 2 introducimos los conceptos a tener en cuenta, no sólo para entender el funcionamiento de HiRaC, sino también para comprender el análisis de seguridad que realizamos. En el capitulo 3 mostramos cómo utilizar la estructura de HiRaC para plantear un un ataque basado en la solución de un problema de rango mínimo. Específicamente, utilizamos el "ruido" de HiRaC, el cual es un polinomio de grado bajo, para hallar una combinación lineal de las matrices de la llave pública que posee rango bajo. Además, logramos asociar el problema de rango mínimo cúbico con los llamados sistemas de Kipnis y Shamir, esto nos permite basarnos en trabajos previos (como [VBC$^+$19]) para estudiar la complejidad del problema de rango mínimo para HiRaC. Luego explicamos cómo usar los resultados del problema de rango mínimo para romper la encriptación de HiRaC. Aquí es importante decir que a pesar que en otros criptosistemas es posible hallar una llave privada equivalente, para HiRaC lo que logramos es explicar una manera de invertir eficientemente la encripción del criptosistema.

En el capítulo 4, hacemos un análisis de la complejidad de resolver el problema de rango mínimo para HiRaC basándonos en resultados experimentales y análisis teórico. Finalmente, basados en la complejidad del ataque planteamos parámetros que garanticen un cierto nivel de seguridad. Basados en este análisis concluimos que es posible escoger parámetros para hacer HiRaC seguro frente al ataque de rango mínimo.

Capítulo 1

El problema de rango mínimo

En este capitulo explicaremos el problema de rango mínimo. Este problema fue introducido por Buss et al. [BSFOS99] y prueba que es un problema NP-completo.

El problema de rango mínimo tiene muchas aplicaciones en el área de la criptografía, siendo una de las más importantes el estudio de la seguridad de criptosistemas basados en polinomios multivariados. En [KS99] Kipnis y Shamir prueban cómo realizar un ataque al criptosistema HFE basado en el problema de rango mínimo. Algunas generalizaciones de este ataque se han realizado para otros criptosistemas, tales como ZHFE [CSTV17] y Multi-HFE [BFP11].

1.1. El problema de rango mínimo cuadrático

El problema de rango mínimo se define como

Problema de rango mínimo, versión decisional

Dados enteros positivos n, r, k y matrices $M_1, ..., M_k \in \mathbb{F}^{n \times n}$, determinar si existen $\lambda_1, ..., \lambda_r \in \mathbb{F}$ tales que el rango de

$$M = \sum_{i=1}^{n} \lambda_i M_i$$

es menor o igual a r.

Se puede probar que este problema es NP-completo e incluso si se asume que las clases computacionales P y NP no son iguales, podemos afirmar que no existe un algoritmo en tiempo polinomial que pueda resolver el problema de rango mínimo para cualquier elección de parámetros. Sin embargo, existen algoritmos que pueden resolver este problema para la elección de ciertos parámetros. En efecto discutiremos algunos algoritmos que pueden hacer esto en tiempo razonable cuando el parámetro r es suficientemente pequeño.

Dada la naturaleza de este trabajo estamos más interesados en la versión de búsqueda del problema de rango mínimo.

Problema del rango mínimo, versión de búsqueda

Dados enteros positivos n, r, k y matrices $M_1, ..., M_k \in \mathbb{F}^{n \times n}$, encontrar $\lambda_1, ..., \lambda_k \in \mathbb{F}$ tales que el rango de

$$M = \sum_{i=1}^{k} \lambda_i M_i$$

es menor o igual a r.

1.2. Algoritmos para resolver el problema de rango mínimo cuadrático

La aproximación básica para resolver el problema de rango mínimo es considerar los coeficientes λ_i como variables y utilizar el hecho de que el rango de $\sum_{i=1}^{n} \lambda_i M_i$ es menor que r, junto con alguna caracterización del rango de una matriz para plantear algún sistema de ecuaciones. Este sistema de ecuaciones será un sistema de polinomios multivariados y no será precisamente fácil resolverlo excepto para algunos parámetros.

1.2.1. Usando la descomposición factorial

Recuerde que el rango de una matriz $A \in \mathbb{F}^{n \times n}$ puede ser definido como el mínimo número de sumandos r tal que A puede ser escrita como $A = \sum_{i=1}^{r} \mathbf{u}_i \mathbf{v}_i^{\intercal}$. Tratando cada entrada de $\mathbf{u}_i, \mathbf{v}_i$ como variables, podemos obtener un sistema de n^2 ecuaciones y $2 \cdot r \cdot n + k$ variables.

1.2.2. Modelamiento por menores

En [FLDVP08] Faugère et al. presentaron el método de menores para resolver el problema de rango mínimo. Este método utiliza la caracterización de rango usando menores: el rango de A es a lo más r si y sólo si cada menor de tamaño $r + 1$ es cero. Recordemos que el menor de tamaño l de una matriz es el determinante de una submatriz de $l \times l$ formado de un subconjunto de l filas y l columnas de la matriz A.

Aplicando esta aproximación a la matriz M definida anteriormente, podemos obtener una ecuación por cada menor igualando a cero. Cada una de estas ecuaciones es homogénea de grado $r + 1$ y el número de $r + 1$- menores en M está dado por $\binom{n}{r+1}^2$.

1.2.3. El Método de Kipnis y Shamir

Introducido por Kipnis y shamir en [KS99], el método KS se basa en el siguiente hecho: una matriz M de $n \times n$ posee rango menor o igual a r si y sólo si la dimensión de su kernel por la derecha es por lo menos $n - r$. Esto es equivalente a la existencia de por lo menos

$n - r$ vectores linealmente independientes en el kernel de M. Con alta probabilidad, los vectores del kernel pueden ser escritos de la forma

$$\begin{bmatrix} I_{n-r} \\ K^t \end{bmatrix},$$

donde

$$K = \begin{bmatrix} \alpha_{11} & \dots & \alpha_{1r} \\ \vdots & \ddots & \vdots \\ \alpha_{(n-r)1} & \dots & \alpha_{(n-r)r} \end{bmatrix}$$

y I_{n-r} es la identidad de tamaño $n - r$. Los α_i son variables desconocidas.

Suponiendo que estos vectores están en el kernel de M podemos plantear la ecuación

$$M \begin{bmatrix} I_{n-r} \\ K^t \end{bmatrix} = 0,$$

que deriva en $n(n-r)$ ecuaciones en $k + r(n-r)$ incógnitas, conocido comúnmente como sistema KS$(n \times n, k, r)$.

En [VBC+19] se analiza la estructura de los sistemas KS$(p \times q, m, r)$ y se establece una cota para la complejidad de este sistema de ecuaciones. Esta cota está dada por

$$O\left(\binom{r' + d_{ks} + 1}{d_{ks} + 2}^w\right),$$

donde

$$d_{ks} = \min\left\{d \mid \left[\binom{r}{d}p > \binom{r}{d+1}m\right], 1 \leq d \leq r-1\right\}$$

1.3. Rango de una matriz cúbica

En esta sección explicaremos algunos conceptos relacionados con el rango de una matriz cúbica. Esto se hace necesario no solo para entender mejor el problema de rango mínimo cúbico, sino también para plantear algunos algoritmos para resolverlo. Tambien exhibiremos la relación entre los polinomios cúbicos y las matrices tres dimensionales.

Sea p un polinomio cúbico multivariado en $\mathbb{F}[x_1, \dots, x_n]$, donde $\mathbb{F}$ es un campo finito. La parte homogénea de mayor grado de p puede ser escrita como

$$\sum_{1 \leq i,j,k \leq n} a_{ijk} x_i x_j x_k,$$

donde $a_{ijk} \in \mathbb{F}$. La matriz cúbica A, cuya entrada (i, j, k) está dada por a_{ijk}, se conocerá como la matriz asociada a la parte cúbica homogénea de p.

Denotaremos por $A[i, j, k]$ la entrada (i, j, k) de la matriz A. Además, denotaremos por $A[i, \cdot, \cdot]$ la matriz dos dimensional cuyas entradas están dadas por a_{ijk} donde i es fijo. La matriz $A[i, \cdot, \cdot]$ será conocida como $i-$ésima tajada de la matriz A.

Recordemos que, dada una matriz $A \in \mathbb{F}^{n\times m}$, podemos definir el rango como el mínimo número de sumandos r que nos permiten escribir A como

$$A = \sum_{i=1}^{r} \mathbf{u}_i \mathbf{v}_i^{\intercal},$$

donde $\mathbf{u}_i \in \mathbb{F}^n$ y $\mathbf{v}_i \in \mathbb{F}^m$ para todo $i = 1, \ldots, r$. Teniendo en cuenta que $\mathbf{u}_i\mathbf{v}_i^{\intercal} = \mathbf{u}_i \otimes \mathbf{v}_i$, podemos generalizar esta definición para matrices tres dimensionales. El rango de una matriz tres dimensional $A \in \mathbb{F}^{n\times m\times \ell}$ es el minimo de sumandos r requeridos para escribir A como

$$A = \sum_{i=1}^{r} \mathbf{u}_i \otimes \mathbf{v}_i \otimes \mathbf{w}_i,$$

donde $\mathbf{u}_i \in \mathbb{F}^n$, $\mathbf{v}_i \in \mathbb{F}^m$ y $\mathbf{w}_i \in \mathbb{F}^\ell$ para todo $i = 1, \ldots, r$. Igual que el caso cuadrático, denotamos este número como $\mathsf{rank}(A)$.

Un importante hecho acerca del número $\mathsf{rank}(A)$ es que es siempre finito, y está acotado por n^2. Para ver esto, notemos que podemos escribir

$$A = \sum_{i,j,k} A[i,j,k] \cdot (\mathbf{e}_i \otimes \mathbf{e}_j \otimes \mathbf{e}_k) = \sum_{i} \mathbf{e}_i \otimes \left(\sum_{j,k} A[i,j,k] \cdot (\mathbf{e}_j \otimes \mathbf{e}_k) \right).$$

Ahora, cada matriz cuadrática $\sum_{j,k} A[i,j,k] \cdot (\mathbf{e}_j \otimes \mathbf{e}_k)$ tiene rango a lo más n y entonces tenemos que $\sum_{\ell=1}^{n} \mathbf{u}_\ell^i \otimes \mathbf{v}_\ell^i$, lo cual implica que podemos escribir

$$A = \sum_{i,\ell} \mathbf{e}_i \otimes \mathbf{u}_\ell^i \otimes \mathbf{v}_\ell^i.$$

donde esta suma tiene a lo más n^2 sumandos. Concluimos entonces que $\mathsf{rank}(A) \leq n^2$.

Sabemos que una matriz $\mathbb{F}^{n\times n}$ puede tener rango a lo más n, y más aún, este máximo es alcanzable (por ejemplo, la matriz identidad). Sin embargo, determinar el máximo rango de una matriz cúbica y alcanzarlo, sigue siendo un problema abierto. Arriba, nosotros mostramos que este máximo está acotado por n^2, sin embargo, el máximo es más pequeño que n^2. La mejor aproximación que se conoce para el máximo rango de una matriz en $\mathbb{F}^{n\times n\times n}$, es que esté está entre $(1/3)n^2$ y $(3/4)n^2$ [How78, Theorem 7].

Al igual que el caso cuadrático, existen algunas caracterizaciones que nos permiten diseñar algoritmos para resolver el problema del rango mínimo cúbico. Una de las más útiles para el propósito de este trabajo está dada por el siguiente teorema.

Teorema 1.3.1. *[EO+] Dada una matriz 3-dimensional $M \in \mathbb{F}^{n\times m\times l}$, el rango de M es el mínimo número r de matrices de rango uno $S_1, \ldots, S_r \in \mathbb{F}^{m\times l}$, tales que, para todos las tajadas $M[i,\cdot,\cdot]$ de M, $M[i,\cdot,\cdot] \in \mathrm{span}(S_1, \ldots, S_r)$.*

También vale la pena aclarar que algunas propiedades que satisface el rango de una matriz cuadrada se cumplen para el rango de una matriz cúbica. Una de ellas, y muy útil en este trabajo, es que el rango de una matriz cúbica es invariante bajo transformaciones lineales.

Otro concepto de vital importancia es el siguiente

Definición 1.3.1. Sea $S \in \mathbb{F}^{n\times n\times n}$ una matriz tres dimensional simétrica.[1] Definimos el rango simétrico de S como el mínimo número de sumandos s que se necesitan para escribir S como

$$S = \sum_{i=1}^{s} t_i \mathbf{u}_i \otimes \mathbf{u}_i \otimes \mathbf{u}_i,$$

donde $\mathbf{u}_i \in \mathbb{F}^n$, $t_i \in \mathbb{F}$. Si esta descomposición no existe, se define este número como ∞. Denotamos este número por $\mathsf{SRank}(S)$.

Es claro de la definición de rango y rango simétrico de una matriz $A \in \mathbb{F}^{n\times n\times n}$, que se cumple que $\mathsf{rank}(A) \leq \mathsf{SRank}(A)$. Se puede demostrar que estos números coinciden en algunos casos, pero no siempre [CGLM08].

La siguiente proposición nos garantiza que dada una matriz en $\mathbb{F}^{n\times n\times n}$ el rango simétrico es finito. Un resultado más general se muestra en [SgS13, Proposition 7.2].

Teorema 1.3.2. *Sea $\mathbb{F}$ un campo finito con $|\mathbb{F}| \geq 3$. Entonces cada tres dimensional matriz $S \in \mathbb{F}^{n\times n\times n}$ puede ser escrita como*

$$S = \sum_{i=1}^{s} t_i \mathbf{u}_i \otimes \mathbf{u}_i \otimes \mathbf{u}_i,$$

donde $\mathbf{u}_i \in \mathbb{F}^n$ y $t_i \in \mathbb{F}$.

1.4. El problema de rango mínimo cúbico

La mayoría de esquemas criptográficos basados en polinomios multivariados están basados en polinomios cuadráticos. Esto conlleva al uso de matrices cuadradas y por tanto entender el problema de rango mínimo cuadrático se hace de suma importancia. Sin embargo, en este trabajo estudiamos la seguridad de un sistema basado en polinomios cúbicos, el cual conlleva a trabajar con matrices cúbicas. Por tanto, se hace necesario explicar el problema de rango mínimo cúbico y algunos algoritmos para solucionarlo.

El problema de rango mínimo cúbico se define como

Problema de rango mínimo cúbico, versión decisional

Dados enteros positivos n, r, k y matrices $M_1, ..., M_k \in \mathbb{F}^{n\times n\times n}$, determine si existen $\lambda_1, ..., \lambda_r$ tales que el rango de

$$M = \sum_{i=1}^{n} \lambda_i M_i$$

es menor o igual a r.

Podemos probar que este problema es NP-completo [HL13]. Al igual que la versión cuadrática estamos interesados en la versión de búsqueda del problema.

[1] Una matriz cúbica es simétrica si es invariante ante cualquier permutación de sus índices

Problema del rango mínimo cúbico, versión de búsqueda

Dados enteros positivos n, r, k y matrices $M_1, ..., M_k \in \mathbb{F}^{n\times n}$, encuentre $\lambda_1, ..., \lambda_k \in \mathbb{F}$ tales que el rango de

$$M = \sum_{i=1}^{k} \lambda_i M_i$$

es menor o igual a r.

1.4.1. Algoritmos para el problema de rango mínimo cúbico

Al igual que en el caso cuadrático, se pueden plantear varios algoritmos para resolver el problema de rango mínimo cúbico. Un importante hecho a aclarar es el siguiente, dado un polinomio cúbico con grado acotado por algún D, la matriz asociada a este polinomio tendrá rango acotado por r^2, donde $r = \log_q\left(\frac{D}{3}\right)$. Este hecho es importante en el sentido que el rango de una matriz será acotado por el cuadrado de algún número entero y este parámetro puede agregar más complejidad en los algoritmos planteados para el problema de rango mínimo cúbico.

1.4.2. Usando la descomposición tensorial

La primera aproximación que se puede usar proviene de la definición de rango cúbico. Este algoritmo es similar al presentado en la sección 1.2.1. Sea $A = t_1M_1+\cdots+t_kM_k$, donde las t_i's son variables (así cada entrada de A es un polinomio lineal en las t_i's). Sabemos que $\mathsf{rank}(A) \leq r$ si y solo si existe $\mathbf{u}_i, \mathbf{v}_i, \mathbf{w}_i \in \mathbb{F}^n$ para $i = 1, \ldots, r$ tal que $A = \sum_{i=1}^{r} \mathbf{u}_i \otimes \mathbf{v}_i \otimes \mathbf{w}_i$. Tomando cada $\mathbf{u}_i, \mathbf{v}_i, \mathbf{w}_i$ como un vector de incógnitas obtenemos n^3 ecuaciones cúbicas. El número total de variables está dado por $3 \cdot n \cdot r + k$.

1.4.3. Generalización del método de Kipnis y Shamir

Sabemos del teorema 1.3.1 que una matriz $M \in \mathbb{F}^{n\times n\times n}$ tiene rango r si y sólo si, existen r matrices de rango uno $S_1, \ldots, S_r \in \mathbb{F}^{n\times n}$ tales que

$$M[i, \cdot, \cdot] \in \mathrm{span}(S_1, \ldots S_r).$$

Donde cada matriz S_i tiene rango uno. Podemos escribir

$$S_i = u_i \otimes v_i,$$

para algún $u_i, v_i \in \mathbb{F}^n$. Si tomamos las entradas de cada u_i y v_i como variables desconocidas podemos plantear el sistema de n^3 ecuaciones

$$\sum_{i=1}^{n} \alpha_{ij} u_i \otimes v_i = M[j, \cdot, \cdot] \quad \text{para} \quad j = 1, \cdots, n, \tag{1.1}$$

con $r(2n) + rn + k = 3rn + k$ variables.

En el caso $r \ll n$ se tiene que con alta probabilidad las primeras r tajadas de M serán linealmente independientes y por tanto $\text{span}(S_1, \ldots, S_r) = \text{span}(M[1,\cdot,\cdot], \ldots, M[r,\cdot,\cdot])$. Entonces para $i = r+1, \ldots, n$ se tiene que

$$M[i,\cdot,\cdot] \in \text{span}(M[1,\cdot,\cdot], \ldots, M[r,\cdot,\cdot])$$

y por tanto

$$\sum_{i=1}^{r} \alpha'_{ij} M[i,\cdot,\cdot] = M[j+1,\cdot,\cdot] \quad \text{para} \quad j = r, \cdots, n-1. \tag{1.2}$$

Este es un sistema de $n^2(n-r)$ ecuaciones en $(n-r)r + k$ variables. En la sección 3.4 probamos que este sistema es equivalente a un sistema $\text{KS}(n^2 \times n, k, r)$ y por tanto podemos analizar la complejidad de resolver un problema de rango mínimo cúbico a partir de los resultados obtenidos en [VBC+19].

1.4.4. Tajadas y Diferenciales

Dado un polinomio cúbico $f \in \mathbb{F}[x_1, \ldots, x_n]$, definimos el diferencial de f en $\mathbf{a} \in \mathbb{F}^n$ como

$$D_{\mathbf{a}}(f(\mathbf{x})) := f(\mathbf{x}+\mathbf{a}) - f(\mathbf{x}) - f(\mathbf{a}). \tag{1.3}$$

En [EO+] se muestra que existe una relación entre las tajadas de la matriz cúbica M asociada al polinomio f y los diferenciales de este polinomio.

En efecto, sea $\mathbf{a} \in \mathbb{F}^n$, se puede probar que el diferencial de f en $\mathbf{a}$ está dado por

$$D_{\mathbf{a}} f(\mathbf{x}) = \sum_{i=1}^{n} a_i M[\cdot,\cdot,i].$$

Esto implica que el rango del diferencial está acotado por el rango de la matriz M.

Entonces para solucionar el problema de rango mínimo cúbico bastaría con solucionar un problema de rango mínimo cuadrático obtenido a partir de los diferenciales. Este aproximamiento no necesariamente hace el problema más fácil y en algunos casos no resulta efectivo, como el caso de HiRaC que veremos más adelante.

Capítulo 2

Criptografía de llave pública multivariada

Los criptosistemas de llave pública multivariada (MPKC) pertenece a la rama de criptografía de llave pública. Es decir, el criptosistema se basa en poseer dos tipos de llaves, una pública y una privada. A continuación describiremos el funcionamiento general de un criptosistema de clave pública para entender mejor los sistemas MPKC.

Supongamos que **Alice** posee un mensaje m y quiere que **Bob** pueda leerlo pero garantizando que nadie más, excepto Bob pueda hacerlo.

Para resolver este problema, suponga que tenemos una función $\mathcal{P}$ tal que

1. $\mathcal{P}$ es uno a uno.

2. $\mathcal{P}$ es fácil de evaluar para cualquiera que quiera enviar un mensaje a Bob.

3. $\mathcal{P}$ no es fácil de invertir para cualquiera que simplemente conozca $\mathcal{P}$.

4. Bob posee alguna información secreta que le permite invertir fácilmente a $\mathcal{P}$.

Las primeras tres propiedades garantizan que $\mathcal{P}$ es una función one-way y la última que es una función de puerta trasera. En [KL07] se encuentran más detalles de estos conceptos.

Lo que hace Alice para resolver su problema es tomar el mensaje m y evaluar $\mathcal{P}(m)$. Entonces ella envía este valor a Bob, y a partir de las propiedades de $\mathcal{P}$ obtener el mensaje m. A continuación, introducimos algunos conceptos esenciales en criptografía.

- La función $\mathcal{P}$ es conocida como llave pública y es conocida por cualquiera que quiera enviar un mensaje a Bob.

- La información secreta para invertir $\mathcal{P}$ es conocida como llave privada.

- Todo mensaje m en el dominio de $\mathcal{P}$ es conocido como texto plano y todo elemento en su rango como texto cifrado.

- Encriptar es el acto de evaluar la función $\mathcal{P}$ y desencriptar es el acto de invertir esta función.

La manera general en que una función de puerta trasera $\mathcal{P}$ es construida es a través de un algoritmo Gen que toma una información secreta sk y da como resultado una función de puerta trasera que puede ser invertida a partir de sk.

Ejemplo.(RSA) Considere dos números primos p y q, dos números enteros positivos tales que $ed \equiv 1 \mod \phi(pq)$, donde ϕ es la función de Euler. Podemos demostrar que para todo m entre 1 y $n-1$ se cumple que

$$(m^e)^d = m^{ed} = m^1 \mod pq.$$

Sea $\mathcal{P}$ la función que toma m y calcula su $e-$th potencia módulo pq. Se acepta que hallar m directamente de $\mathcal{P}(m)$ es difícil, pero si se conoce el número d simplemente hay que calcular $m = \mathcal{P}(m)^d$. Si tomamos d como la información secreta, solo quien conozca esta información es capaz de desencriptar el mensaje m. más aún, encontrar d es equivalente a encontrar p y q que son la factorización del entero pq, así la seguridad de este criptosistema se basa en la dificultad de factorizar grandes números.

2.1. Generalidades de los criptosistemas basados en polinomios multivariados

En 1988, T. Matsumoto and H. Imai [MI88] presentaron el criptosistema llamado C^*, el cual fue roto por Jacques Patarin en 1996 [Pat95] a través de una técnica llamada relinearización y a su vez propuso un sistema de encripción llamado HFE (Hidden Field Equation), el cual está basado en polinomios multivariados cuadráticos sobre campos finitos. Aunque HFE se probó inseguro debido a un ataque de rango mínimo, muchos de los criptosistemas MPKC se basan en su idea. En esta sección mostraremos la idea general detrás de la construcción de un sistema MPKC.

Durante el resto de este documento, $\mathbb{F}$ denotará un campo finito con q elementos, $\mathbb{K}$ una extensión de $\mathbb{F}$ de grado n y $R = \mathbb{F}[x_1, ..., x_n]$ el anillo de polinomios con coeficientes en $\mathbb{F}$.

Consideremos el siguiente problema computacional.

Problema MP. Sean $p_1, ..., p_n \in R$ polinomios multivariados escogidos aleatoriamente. Encontrar $a \in \mathbb{F}^n$, tal que para todo $i = 1, ..., n$

$$p_i(a) = 0.$$

Hay muchas razones para creer que este problema es difícil de resolver incluso para computadores cuánticos, de hecho, el problema de decidir cuando un sistema de polinomios tiene una solución o no es NP-completo [GJ02]. Este problema se convierte en el punto de partida de los sistemas MPKC, en estos criptosistemas la llave pública está dada por una $n-$tupla de polinomios $(p_1(x), ..., p_n(x))$ y encriptar un mensaje m es evaluarlo en cada polinomio, entonces el texto cifrado sería la $n-$tupla $c = (c_1, ..., c_n)$ donde

$$c_i = p_i(m) \qquad \text{para } i = 1, .., n.$$

Ahora sea $c = (c_1, ..., c_n)$ un texto cifrado, sabemos que $c_i = p_i(m)$, para algún mensaje m. Entonces hallar el mensaje m es equivalente a resolver una instancia del problema MQ con los polinomios cuadráticos $q_i = p_i(m) - c_i$. Claramente este problema no es NP-completo donde los q_i no son elegidos aleatoriamente, pero pruebas experimentales muestran que este problema es difícil también con la correcta elección de los polinomios. En general para construir un sistema MPKC podemos resumirlo de la siguiente manera.

1. Escogemos una función $P : \mathbb{F}^n \to \mathbb{F}^m$, donde

$$P(X) = (p_1(X), ..., p_m(X))$$

   y el sistema de ecuaciones $p_1(X) = y_1, ..., p_m(X) = y_m$ es solucionado eficientemente.

2. Escogemos mapeos lineales $L_1 : \mathbb{F}^m \to \mathbb{F}^m$, $L_2 : \mathbb{F}^n \to \mathbb{F}^n$.

3. La llave pública está dada por la composición

$$L_1 \circ P \circ L_2$$

   y la llave privada consiste en las funciones L_1, P, L_2.

De acuerdo a la sección anterior, queremos una forma de construir P de tal manera que exista una información secreta que nos permita invertir fácilmente $L_i \circ P \circ L_2$. Para esto consideremos el mapeo $\phi : \mathbb{K} \to \mathbb{F}$ definido como

$$\phi(a_0 + a_1 x + ... + a_n x^n) = (a_1, ..., a_n).$$

Ahora, dado dos números a y b definimos el $b-$peso de Hamming de a como la suma de los coeficientes de la expansión de a en base b.

Definición 2.1.1. El peso de un monomio $X^a \in \mathbb{K}[X]$ es el $q-$peso de Hamming de a. Un polinomio $\mathcal{F} \in \mathbb{K}$ se dice que es homogéneo de peso d si todos sus monomios tienen peso d y se dice que es de peso d si todos sus monomios tienen peso a lo más d.

El siguiente teorema garantiza que al tomar un polinomio $\mathcal{F} \in \mathbb{K}$ podemos construir una tupla de polinomios multivariados sobre $\mathbb{F}$.

Teorema 2.1.1. *[EO+] Sea $d \geq 0$ un entero, sea $\mathbb{K}_d[X]$ el conjunto de polinomios homogéneos de grado d en $\mathbb{K}[X]$ de peso d y sea R_d^n el conjunto de funciones $F : \mathbb{F}^n \to \mathbb{F}^n$ cuyas coordenadas son polinomios homogéneos de grado d en R. Entonces la siguiente biyección está bien definida*

$$\begin{aligned} \mathsf{Drp} : \mathbb{K}[X]_d &\longrightarrow R_d^n \\ \mathcal{F} &\longrightarrow \phi \circ \mathcal{F} \circ \phi^{-1}. \end{aligned}$$

cuya función inversa está dada por

$$\begin{aligned} \mathsf{Lft} : R_d^n &\longrightarrow \mathbb{K}[X]_d \\ \mathcal{F} &\longrightarrow \phi^{-1} \circ \mathcal{F} \circ \phi. \end{aligned}$$

Entonces, al tomar un polinomio $\mathcal{F} \in \mathbb{K}[X]$ de peso d, podemos obtener una tupla de polinomios multivariados sobre $\mathbb{F}$ que serán la llave pública del sistema MPKC. La llave privada estará constituida por la función $\mathcal{F}$, la cual es escogida adecuadamente para hacer eficiente la búsqueda de imagenes inversas.

Comúnmente se escoge $d = 2$ por dos razones principalmente.

- Existen $O(n^d)$ monomios de grado d, por lo que necesitamos $O(mn^d)$ elementos de $\mathbb{F}$ para guardar m polinomios en R de grado d. Para $d = 2$ esta es una cantidad manejable.
- Necesitamos computar Drp$(\mathcal{F})$ de una manera eficiente y existe una manera de hacerlo en el caso cuadrático.

2.2. Computación del Droping y Lifting en el caso cuadrático.

La función Drp descrita en el teorema 2.1.1 se conoce como el Droping (bajada) de un polinomio $\mathcal{F} \in \mathbb{K}$. Igualmente la función Lft se conoce como el Lifting(levantamiento) de una tupla de polinomios en R. El droping es una de las partes más importantes en la criptografía de polinomios multivariados, dado que es la que permite obtener la llave pública. En esta sección, explicaremos como obtener el droping de un polinomio de peso 2 en $\mathbb{K}$ y el lifting de polinomios cuadráticos en R.

Sea $p(x_1, \ldots, x_n) \in R$ un polinomio cuadrático, entonces p tiene la forma

$$p(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j + \sum_{i=1}^{n} b_i x_i + c$$

y entonces podemos escribirlo como

$$p(x_1, \ldots, x_n) = \mathbf{x}^\intercal A \mathbf{x} + B\mathbf{x} + c$$

donde $\mathbf{x} = [x_1, \ldots, x_n]^\intercal$, $A \in \mathbb{F}^{n \times n}$ es la matriz $[a_{ij}]_{ij}$ y $B \in \mathbb{F}^{1 \times n}$ es la matriz $[b_i]_{1i}$. En algunos casos nos referiremos a A como la matriz asociada a la parte cuadrática del polinomio.

Podemos hacer algo similar para los polinomios en $\mathbb{K}[X]$ que poseen peso 2. Estos polinomios tienen la forma

$$\mathcal{F}(X) = \sum_{i,j=1}^{n} \alpha_{ij} X^{q^{i-1}+q^{j-1}} + \sum_{i=1}^{n} \beta_i X^{q^{i-1}} + \gamma$$

por tanto, podemos escribirlos como

$$\mathcal{F}(X) = \mathbf{X}^\intercal M \mathbf{X} + N\mathbf{X} + \gamma$$

donde $\mathbf{X} = [X^{q^0}, \ldots, X^{q^{n-1}}]^\intercal$, $M \in \mathbb{K}^{n \times n}$ es la matriz $[\alpha_{ij}]_{ij}$ y $N \in \mathbb{K}^{1 \times n}$ es la matriz $[\beta_i]_{1i}$. M comúnmente es llamada matriz asociada al polinomio $\mathcal{F}$.

Para lo que sigue necesitamos la siguiente matriz

$$\Delta = \begin{bmatrix} y^0 & y^1 & \cdots & y^{n-2} & y^{n-1} \\ (y^0)^{q^1} & (y^1)^{q^1} & \cdots & (y^{n-2})^{q^1} & (y^{n-1})^{q^1} \\ (y^0)^{q^2} & (y^1)^{q^2} & \cdots & (y^{n-2})^{q^2} & (y^{n-1})^{q^2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ (y^0)^{q^{n-1}} & (y^1)^{q^{n-1}} & \cdots & (y^{n-2})^{q^{n-1}} & (y^{n-1})^{q^{n-1}} \end{bmatrix}$$

la cual satisface

$$\mathbf{X} = \Delta \cdot \phi(X).$$

Sea $\mathcal{F}(X) \in \mathbb{K}[X]$ un polinomio de peso 2 con la ecuación

$$\mathcal{F}(X) = \mathbf{X}^\intercal M\mathbf{X} + N\mathbf{X} + \gamma,$$

Mostraremos una ecuación para el $\mathsf{Drp}(\mathcal{F})$ en términos de M y N. Si $\mathbf{x} = \phi(X)$, entonces

$$\begin{aligned} \mathcal{F}\left(\phi^{-1}(\mathbf{x})\right) = \mathcal{F}(X) &= \mathbf{X}^\intercal M\mathbf{X} + N\mathbf{X} + \gamma \\ &= (\Delta \cdot \phi(X))^\intercal M\left(\Delta \cdot \phi(X)\right) + N\left(\Delta \cdot \phi(X)\right) + \gamma = \mathbf{x}^\intercal \Delta^\intercal M\Delta\mathbf{x} + N\Delta\mathbf{x} + \gamma. \end{aligned}$$

factorizando los y^i de las matrices $\Delta^\intercal M\Delta$ y $N\Delta$, obtenemos

$$\Delta^\intercal M\Delta = \sum_{i=1}^{n} y^{i-1} A_i$$

y

$$N\Delta = \sum_{i=1}^{n} y^{i-1} B_i$$

donde $A_i \in \mathbb{F}^{n\times n}$ y $B_i \in \mathbb{F}^{1\times n}$, y entonces, sí $\gamma = c_1 + c_2 y + \cdots + c_n y^{n-1}$

$$\begin{aligned} \mathcal{F} \circ \phi^{-1}(\mathbf{x}) = \mathbf{x}^\intercal \left(\sum_{i=1}^{n} y^{i-1} A_i\right)\mathbf{x} + \left(\sum_{i=1}^{n} y^{i-1} B_i\right)\mathbf{x} + \sum_{i=1}^{n} c_i y^{i-1} \\ = \sum_{i=1}^{n} y^{i-1}\left(\mathbf{x}^\intercal A_i\mathbf{x} + B_i\mathbf{x} + c_i\right). \end{aligned}$$

para todo i tenemos que $\mathbf{x}^\intercal A_i\mathbf{x} + B_i\mathbf{x} + c_i \in \mathbb{F}$, y por la definición de ϕ concluimos que

$$\mathsf{Drp}(\mathcal{F})(\mathbf{x}) = \phi \circ \mathcal{F} \circ \phi^{-1}(\mathbf{x}) = \left[\mathbf{x}^\intercal A_1\mathbf{x} + B_1\mathbf{x} + c_1, \ldots, \mathbf{x}^\intercal A_n\mathbf{x} + B_n\mathbf{x} + c_n\right]^\intercal.$$

Sea $F : \mathbb{F}^n \to \mathbb{F}^n$ dado por n polinomios cuadráticos $p_1, \ldots, p_n \in R$, donde cada polinomio p_i tiene la forma

$$p_i(x_1, \ldots, x_n) = \mathbf{x}^\intercal A_i\mathbf{x} + B_i\mathbf{x} + c_i$$

donde $A_i \in \mathbb{F}^{n\times n}$ y $B_i \in \mathbb{F}^{1\times n}$. Mostraremos una forma de obtener el Lft de F a partir de las matrices A_i y N_i.

Definamos $\gamma = c_1 + c_2 y + \cdots + c_n y^{n-1} \in \mathbb{K}$ y las matrices $M \in \mathbb{K}^{n\times n}, N \in \mathbb{K}^{1\times n}$ como

$$M = (\Delta^{\intercal})^{-1} \left(\sum_{i=1}^{n} y^{i-1} A_i \right) \Delta^{-1}$$

y

$$N = \left(\sum_{i=1}^{n} y^{i-1} B_i \right) \Delta^{-1}.$$

revirtiendo los pasos que mostramos para obtener $\mathsf{Drp}\ \mathsf{Lft}(F)$, tenemos que

$$\mathsf{Lft}\,(F)\,(X) = \phi^{-1} \circ \mathcal{F} \circ \phi(X) = \mathbf{X}^{\intercal} M \mathbf{X} + N\mathbf{X} + \gamma.$$

2.3. Computación del Droping en el caso cúbico

A pesar que la mayoría de criptosistemas de llave pública multivariada están basados en polinomios cuadráticos, nosotros podemos utilizar cualquier grado para construir un MPKC. Una de las dificultades al considerar $d > 2$ es que el droping de un polinomio puede no ser fácil de calcular. En [EO+] se muestra una manera sencilla de hacer este cálculo en el caso de polinomio de peso 3 y esto nos permite proponer sistemas que se basen en polinomios cúbicos.

Sea $\mathcal{F} \in \mathbb{K}[X]$ un polinomio homogéneo de peso 3 dado por

$$\mathcal{F}(X) = \sum_{1\le i,j,k\le n} \alpha_{i,j,k} X^{q^{i-1}+q^{j-1}+q^{k-1}}.$$

Nuestro objetivo es dar una forma explícita a los polinomios de la composición $\phi \circ \mathcal{F} \circ \phi^{-1}$. Podemos representar el polinomio $\mathcal{F}$ como $\mathcal{F}(X) = \mathcal{T}(\mathbf{X}, \mathbf{X}, \mathbf{X})$ donde $\mathbf{X} = (X^{q^0}, \ldots, X^{q^{n-1}})^{\intercal}$ y $\mathcal{T} : \mathbb{K}^n \times \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}$ es la forma trilineal dada por

$$\mathcal{T}(\boldsymbol{\beta}, \boldsymbol{\delta}, \boldsymbol{\gamma}) = \sum_{1\le i,j,k\le n} \alpha_{i,j,k} \cdot (\beta_i \delta_j \gamma_k).$$

Sea A la matriz tres dimensional cuya entrada (i, j, k) es dada por $\alpha_{i,j,k}$, y asumamos sin pérdida de generalidad que es una matriz simétrica (en otro caso podemos considerar la matriz cuyas entrada (i, j, k) es dada por $\frac{1}{3!} \cdot (A[i, j, k] + A[i, k, j] + A[j, i, k] + A[j, k, i] + A[k, i, j] + A[k, j, i])$, que representa la misma forma trilineal $\mathcal{T}$).

Sea $\mathcal{T}' : \mathbb{K}^n \times \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}$ la forma trilineal dada por $\mathcal{T}'(\boldsymbol{\beta}, \boldsymbol{\delta}, \boldsymbol{\gamma}) = \mathcal{T}(\Delta\boldsymbol{\beta}, \Delta\boldsymbol{\delta}, \Delta\boldsymbol{\gamma})$, entonces podemos escribir esta forma trilineal como

$$\mathcal{T}'(\boldsymbol{\beta}, \boldsymbol{\delta}, \boldsymbol{\gamma}) = \sum_{1\le i,j,k\le n} \alpha'_{i,j,k} \cdot (\beta_i \delta_j \gamma_k)$$

donde $\alpha'_{i,j,k} = \mathcal{T}'(\mathbf{e}_i, \mathbf{e}_j, \mathbf{e}_k) = \mathcal{T}(\Delta\mathbf{e}_i, \Delta\mathbf{e}_j, \Delta\mathbf{e}_k)$.

Sea $\mathbf{a} \in \mathbb{F}^n$ y tomemos $\alpha = \phi^{-1}(\mathbf{a})$, sabemos que

$$\mathsf{Frob}(\alpha) = (\alpha^{q^0}, \ldots, \alpha^{q^{n-1}}) = \Delta \cdot \phi(\alpha) = \Delta \cdot \mathbf{a}$$

y por tanto

$$\begin{aligned}\mathcal{F}\circ\phi^{-1}(\mathbf{a}) = \mathcal{F}(\alpha) = \mathcal{T}(\mathsf{Frob}(\alpha),\mathsf{Frob}(\alpha),\mathsf{Frob}(\alpha)) = \mathcal{T}(\Delta\cdot\mathbf{a},\Delta\cdot\mathbf{a},\Delta\cdot\mathbf{a})\\ = \mathcal{T}'(\mathbf{a},\mathbf{a},\mathbf{a}) = \sum_{1\le i,j,k\le n}\alpha'_{i,j,k}\cdot(a_ia_ja_k).\end{aligned}$$

Sean $R_1,\ldots,R_n\in\mathbb{F}^{n\times n\times n}$ las matrices simétricas tridimensionales tales que $A' = y^0\cdot R_1 + y^1\cdot R_2+\cdots+y^{n-1}\cdot R_n$, donde $y^0, y^1\ \ldots y^{n-1}$ es la base de $\mathbb{K}$ sobre $\mathbb{F}$. Entonces

$$\begin{aligned}\mathcal{F}\circ\phi^{-1}(\mathbf{a}) &= \sum_{1\le i,j,k\le n}\alpha'_{i,j,k}\cdot(a_ia_ja_k)\\ &= \sum_{1\le i,j,k\le n}\left(\sum_{\ell=1}^{n} y^{\ell-1}R_\ell[i,j,k]\right)\cdot(a_ia_ja_k)\\ &= \sum_{\ell=1}^{n} y^{\ell-1}\underbrace{\left(\sum_{1\le i,j,k\le n}R_\ell[i,j,k]\cdot(a_ia_ja_k)\right)}_{t_\ell}.\end{aligned}$$

donde $t_\ell\in\mathbb{F}$, obtenemos que $\phi\circ\mathcal{F}\circ\phi^{-1}(\mathbf{a}) = (t_1,\ldots,t_\ell)^\intercal$, mas aun, cada polinomio cúbico en la composición $\phi\circ\mathcal{F}\circ\phi^{-1}$ es dado por

$$f_\ell(\mathbf{x}) = \sum_{1\le i,j,k\le n}R_\ell[i,j,k]\cdot(x_ix_jx_k).$$

Nótese que, si A_ℓ es la matriz cuya entrada (i,j,k) es dada por $R_l[i,j,k]$ entonces esta es la matriz cúbica asociada al ℓ-ésimo polinomio en $\phi\circ\mathcal{F}\circ\phi^{-1}$.

2.4. HFE

Recordemos que queremos un polinomio $\mathcal{F}(X)\in\mathbb{K}[X]$ del cual podamos tener una información secreta que nos permita invertir eficientemente este polinomio. En campos finitos hay maneras eficientes de hallar las raíces de un polinomio univariado si su grado es lo suficientemente bajo(por ejemplo el algoritmo de Berlekamp y Cantor-Zassenhaus [LN97]). Con base en esto, es natural escoger polinomios de grado bajo dado que estos son fáciles de invertir.

En HFE, la función central es dada por un polinomio de peso 2 de grado bajo. Mas precisamente, fije un parámetro D y considere el polinomio

$$\mathcal{F}(X) = \sum_{q^i+q^j\le D}\alpha_{ij}X^{q^i+q^j}.$$

$\mathcal{F}$ no necesariamente tiene que ser homogéneo, pero para esta sección lo tomaremos así. Si D es lo suficientemente pequeño, esta función es fácil de invertir. La función de puerta trasera se construye tomando dos transformaciones lineales invertibles $S,T:\mathbb{F}^n\to\mathbb{F}^n$ y computando $P = T\circ\phi\circ\mathcal{F}\circ\phi^{-1}\circ S$.

El criptosistema HFE tiene un vulnerabilidad conocida como el ataque de rango mínimo (Minrank attack). Este ataque reduce el problema de hallar una llave privada equivalente[1] a un problema de rango mínimo.

Empezamos escribiendo el polinomio $\mathcal{F}$ como

$$\mathcal{F}(X) = \begin{pmatrix} X^{q^0} & X^{q^1} & \cdots & X^{q^{n-1}} \end{pmatrix} \begin{pmatrix} * & \cdots & * & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ * & \cdots & * & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} X^{q^0} \\ X^{q^1} \\ \vdots \\ X^{q^{n-1}} \end{pmatrix}$$

donde solamente el cuadrado de $r \times r$ en la parte superior izquierda es no cero ($r = \lfloor \log_q \left(\frac{D}{2}\right) \rfloor$). Denotemos la matriz resultante como $M \in \mathbb{K}^{n \times n}$. Notemos que M tiene un rango bajo r (donde D es pequeño por construcción).

Ahora, de la sección 2.2 tenemos que si $A_i \in \mathbb{F}^{n \times n}$ es la matriz simétrica cuadrada que representa la i-ésima componente de $\mathsf{Drp}(\mathcal{F}) = \phi \circ \mathcal{F} \circ \phi^{-1}$, entonces

$$\Delta^\intercal M \Delta = \sum_{i=1}^{n} y^{i-1} A_i.$$

Es fácil verificar que la composición con la matriz $S \in \mathbb{F}^{n \times n}$ da como resultado

$$\phi \circ \mathcal{F} \circ \phi^{-1} \circ S = (\Delta S)^\intercal M (\Delta S).$$

Finalmente, la matriz P_i asociada a la $i-$ésima componente de $P = T \circ \phi \circ \mathcal{F} \circ \phi^{-1} \circ S$ es dada por

$$P_i = \sum_{j=1}^{n} T[i,j] \cdot (S^\intercal A_j S).$$

Podemos ver que la siguiente relación se cumple

$$(\Delta S)^\intercal M (\Delta S) = \sum_{i=1}^{n} \lambda_i P_i, \tag{2.1}$$

donde $(\lambda_1, \ldots, \lambda_n) = (y^0, \ldots, y^{n-1}) T^{-1}$. Esto último porque

$$\sum_{i=1}^{n} \lambda_i P_i = \sum_{i=1}^{n} \lambda_i \left(\sum_{j=1}^{n} T[i,j] \cdot (S^\intercal A_j S) \right) = \sum_{j} S^\intercal A_j S \sum_{i} \lambda_i T[i,j] = \sum_{j} y^{j-1} S^\intercal A_j S.$$

De la ecuación (2.1) concluimos que el lado derecho tiene el mismo rango que la matriz M, que es a lo más r. Esto nos permite construir una instancia del problema de rango mínimo para realizar un ataque a HFE. Este ataque nos permite encontrar unos coeficientes $\lambda_1, \ldots, \lambda_n$ y usarlos para construir una llave equivalente para este criptosistema (para más detalles véase [BFP13]).

[1] Esto es, unos polinomios con las mismas características a los originales que nos permiten encriptar y desencriptar.

2.5. HiRaC: High Rank Cryptosystem

En la sección 2.1 describimos los sistemas MPKC y establecimos que el estándar a la hora de construir uno de estos criptosistemas es usar polinomios $\mathcal{F} \in \mathbb{K}[X]$ de $q-$peso de Hamming 2. Esto nos permite obtener una tupla de polinomios cuadraditos $\text{Drp}(\mathcal{F}) = \phi \circ \mathcal{F} \circ \phi^{-1}$ en $\mathbb{F}[x_1, \ldots, x_n]$.

El motivo de esta construcción es la eficiencia a la hora de calcular $\text{Drp}(\mathcal{F})$. Sin embargo Escudero [EO+] muestra que al elegir un polinomio de $q-$peso de Hamming 3 en $\mathcal{F} \in \mathbb{K}[X]$ es eficiente calcular $\text{Drp}(\mathcal{F})$. Como resultado se obtiene una tupla de polinomios cúbicos en $\mathbb{F}[x_1, \ldots, x_n]$. Una de las ventajas obtenidas al hacer esto, es que las matrices asociadas a estos polinomios serán cúbicas, lo que implica que los rangos de estas pueden, en teoría, superar el $O(n^2)$ y ser más seguros frente a ataques algebraicos directos.

Con base en esto en [Osp16] se introduce un criptosistema basado en polinomios cúbicos conocido como HiRaC.

Consideremos que q es un número primo mayor a 3. Tomemos un parámetro r lo suficientemente pequeño para garantizar que el mapeo central del sistema sea invertible. Tomemos un polinomio de peso 2, $\mathcal{F} \in \mathbb{K}[X]$. Para cada $j = 0, .., r$ escogemos polinomios aleatorios de peso 1, $\mathcal{M}_j \in \mathbb{K}[X]$ y un polinomio de peso 3, $\mathcal{G}(X) \in \mathbb{K}[X]$ cuya más grande potencia sea $3q^r$. También tomaremos dos transformaciones lineales aleatorias $S, T : \mathbb{F}^n \to \mathbb{F}^n$ y consideraremos el polinomio $\mathcal{H} : \mathbb{K} \to \mathbb{K}$ de peso 3 dado por

$$\mathcal{H}(X) = \sum_{j=0}^{r} X^{q^j} \mathcal{M}_j(\mathcal{F}'(X)) + \mathcal{G}(X), \tag{2.2}$$

donde $\mathcal{F}' = \mathcal{F} \circ \phi^{-1} \circ S^{-1} \circ \phi$. Luego la llave pública será

$$(\phi \circ \mathcal{F} \circ \phi^{-1}, T \circ \phi \circ \mathcal{H} \circ \phi^{-1} \circ S) \tag{2.3}$$

y la privada la tupla $(\mathcal{F}, \mathcal{M}_j, S, T, \mathcal{G}, \mathcal{H})$.

La llave pública se puede dividir en dos partes, una cuadrática dada por la tupla de polinomios $\phi \circ \mathcal{F} \circ \phi^{-1}$ y una cúbica dada por $T \circ \phi \circ \mathcal{H} \circ \phi^{-1} \circ S$.

Para invertir P procederemos de la siguiente manera. Suponga que tenemos un texto cifrado $\mathbf{c} = (c_1, \ldots, c_{2n})$ en el rango de P, y queremos resolver las ecuaciones $\mathcal{F}(\phi^{-1}(\mathbf{x})) = Z_1$, $\mathcal{H}(\phi^{-1}(S\mathbf{x})) = Z_2$ donde $Z_1 = \phi^{-1}(c_1, \ldots, c_n)$ y $Z_2 = \phi^{-1} \circ T^{-1}(c_{n+1}, \ldots, c_{2n})$. Tomando $X = \phi^{-1}(S\mathbf{x})$, esto es lo mismo que $\mathcal{F}'(X) = Z_1$ y $\mathcal{H}(X) = Z_2$. Cualquier solución de este sistema también debe satisfacer la ecuación

$$Z_2 = \sum_{j=0}^{r} X^{q^j} \mathcal{M}_j(Z_1) + \mathcal{G}(X).$$

Un análisis preliminar del rango de $\mathcal{H}$ muestra que posee un rango a lo más $3rn$, el cual podría ser considerado como un rango alto y que motiva el nombre del criptosistema. La función $\mathcal{G}$ es utilizada como ruido, esto es, su propósito es ocultar la composición de las $\mathcal{M}_j$ y $\mathcal{F}$. Más aún, La función $\mathcal{G}$ evita que la función $\mathcal{H}$ tenga caídas de grado bajas.

Definición 2.5.1. Una caída de grado en grado d de una tupla de polinomios $(\mathcal{F}_1, \ldots, \mathcal{F}_n)$ de $q-$peso de Hamming d' en $\mathbb{K}[X]$ es una tupla $(\mathcal{H}_1, \ldots, \mathcal{H}_n) \in (\mathbb{K}[X]_{d-d'})^n$ tal que $\mathcal{H}_1 \mathcal{F}_1 + \cdots + \mathcal{H}_n \mathcal{F}_n$ tiene un $q-$peso de Hamming menor o igual a d.

Las caídas de grado son muy importantes en sistemas MPKC porque permiten establecer una cota de la complejidad que un algoritmo, como F_4 o XL puedan invertir un sistema de polinomios multivariados.

Si retiramos $\mathcal{G}$ de la ecuación (2.2) obtendremos que

$$\mathcal{H}(X) = \sum_{j=0}^{r} X^{q^j} \mathcal{M}_j(\mathcal{F}'(X))$$

y por tanto podemos formular el siguiente resultado (para una demostración ver [Osp16]).

Teorema 2.5.1. *Sean* $(Y_0, Y_1) \in G(X)$ *donde* $G(X) = (\mathcal{F}'(X), \mathcal{H}(X))$*, entonces* $(\mathcal{F}'(X) - Y_0, \mathcal{H}(X) - Y_1)$ *tiene caídas de grado en grado* 3*.*

Esta caída de grado no crece con n por ende tendríamos una debilidad crítica para la versión de HiRaC sin ruido. La función $\mathcal{G}$ tiene un rango bajo para hacer eficiente el proceso de desencripción sin embargo esta característica puede ser usada para atacar HiRaC por medio de un ataque de rango mínimo, como veremos en el capítulo 3.

Capítulo 3

Análisis de seguridad para HiRaC

En este capítulo analizaremos la vulnerabilidad de HiRaC a través de un ataque de rango mínimo. Este ataque es posible dada la estructura de la función central $\mathcal{H}(X)$, la cual involucra una función $\mathcal{G}(X)$ que tiene asociada una matriz de rango bajo. Más específicamente, utilizaremos el hecho de que podemos escribir

$$\mathcal{G}(X) = \mathcal{H}(X) - \sum_{j=0}^{r} X^{q^j} \mathcal{M}_j(\mathcal{F}'(X))$$

y entonces hallar una combinación lineal de polinomios de la llave pública que conlleva a una matriz de rango bajo.

En la primera sección describimos cómo obtener la combinación lineal de matrices de rango bajo y los parámetros del ataque de rango mínimo. Luego procedemos a analizar cómo resolver este problema de rango mínimo, desde su parte cuadrática y cubica. Por último describimos cómo obtener una llave equivalente de HiRaC en el supuesto de tener éxito en el ataque.

3.1. Ataque de rango mínimo para HiRaC

Nuestro objetivo es encontrar una combinación lineal de las matrices asociadas a los polinomios de la llave pública que posea rango bajo y que nos permita encontrar información de la llave privada de HiRaC. Para lograr esto utilizaremos la ecuación

$$\mathcal{G}(X) = \mathcal{H}(X) - \sum_{j=0}^{r} X^{q^j} \mathcal{M}_j(\mathcal{F}'(X)) \tag{3.1}$$

obtenida gracias a la construcción de la función central $\mathcal{H}(X)$ y el siguiente resultado.

Lema 3.1.1. *[EO+] Sea $\mathbb{K} = \mathbb{F}[y]/\langle g(y)\rangle$ donde $g(y) = a_0 + a_1 y + \ldots + a_n y^{n-1} + y^n$ es un polinomio irreducible sobre $\mathbb{F}$. Sea*

$$C = \begin{bmatrix} 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \dots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -a_{n-1} \end{bmatrix},$$

entonces para cualquier $\alpha \in \mathbb{K}$ *tenemos que* $\phi(\alpha y^j) = C^j \cdot \phi(\alpha)$.

Para $\mathbf{x} \in \mathbb{F}^n$, sea

$$\phi \circ \mathcal{F} \circ \phi^{-1}(\mathbf{x}) = (p_0(\mathbf{x}), \dots, p_{n-1}(\mathbf{x}))$$

la primera parte de la llave pública de HiRaC. Dado que cada función M_j posee q-peso 1 en $K[X]$, la $n-$tupla de funciones $\phi \circ M_j \circ \phi^{-1}$ está compuesta por funciones lineales sobre $\mathbb{F}$, más aún, la $i-$ésima componente de $\phi \circ M_j \circ \phi^{-1}(\mathbf{x})$ puede ser expresada como

$$(\phi \circ \mathcal{M}_j \circ \phi^{-1}(\mathbf{x}))_i = \sum_{k=0}^{n-1} \lambda_{jik} x_k + c_{ij},$$

entonces

$$\begin{aligned} \phi \circ \mathcal{M}_j \circ \mathcal{F} \circ \phi^{-1}(\mathbf{x}) &= \phi \circ \mathcal{M}_j \circ \phi^{-1} \circ \phi \circ F \circ \phi^{-1}(\mathbf{x}) \\ &= \phi \circ \mathcal{M}_j \circ \phi^{-1}(p_0(\mathbf{x}), \dots, p_{n-1}(\mathbf{x})) \\ &= \left(\sum_{k=0}^{n-1} \lambda_{j0k} p_k(\mathbf{x}) + c_{1j}, \dots, \sum_{k=0}^{n-1} \lambda_{j(n-1)k} p_k(\mathbf{x}) + c_{nj} \right). \end{aligned}$$

Si realizamos el cambio de variable $\mathbf{z} = S^{-1} \circ \phi(X)$, podemos entonces escribir

$$\begin{aligned} \mathcal{M}_j(\mathcal{F}'(X)) &= \phi^{-1} \circ \phi(\mathcal{M}_j \circ \mathcal{F} \circ \phi^{-1} \circ S^{-1} \phi(X)) \\ &= \phi^{-1}(\phi \circ \mathcal{M}_j \circ \mathcal{F} \circ \phi^{-1}(\mathbf{z})) \\ &= \left[\sum_{k=0}^{n-1} \lambda_{j0k} p_i(\mathbf{z}) + c_{1j} \right] + \dots + \left[\sum_{k=0}^{n-1} \lambda_{j(n-1)k} p_n(\mathbf{z}) + c_{nj} \right] y^{n-1}. \end{aligned}$$

A partir del lema 3.1.1 podemos escribir la composición $\mathcal{M}_j(\mathcal{F}'(X))X^{q^j}$ sobre $\mathbb{F}$ de la siguiente manera

$$\begin{aligned} \phi(\mathcal{M}_j(\mathcal{F}'(X))X^{q^j}) &= \phi\left(\left[\sum_{k=0}^{n-1} \lambda_{j0k} p_k(\mathbf{z}) + c_{1j} \right] X^{q^j} + \dots + \left[\sum_{k=0}^{n-1} \lambda_{j(n-1)k} p_k(\mathbf{z}) + c_{nj} \right] y^{n-1} X^{q^j} \right) \\ &= \left[\sum_{k=0}^{n-1} \lambda_{j0k} p_i(\mathbf{z}) + c_{1j} \right] \phi(X^{q^j}) + \dots + \left[\sum_{k=0}^{n-1} \lambda_{j(n-1)k} p_n(\mathbf{z}) + c_{nj} \right] \cdot C^{n-1} \cdot \phi(X^{q^j}) \\ &= \sum_{i=0}^{n-1} \left[\sum_{k=1}^{n} \lambda_{jik} p_k(\mathbf{z}) + c_{ij} \right] \cdot C^i \cdot \phi(X^{q^j}). \end{aligned}$$

De la ecuación (3.1) obtenemos

$$\mathcal{G}(X) = \mathcal{H}(X) - \sum_{j=0}^{r} \mathcal{M}_j(\mathcal{F}'(X))X^{q^j}$$

$$\phi(\mathcal{G}(X)) = \phi(\mathcal{H}(X)) - \sum_{j=0}^{r} \phi(\mathcal{M}_j(\mathcal{F}'(X))X^{q^j})$$

$$\phi \circ \mathcal{G} \circ \phi^{-1} \circ S(\mathbf{z}) = \phi \circ \mathcal{H} \circ \phi^{-1} \circ S(\mathbf{z}) - \sum_{j=0}^{r} \left[\sum_{i=0}^{n-1} \left[\sum_{k=0}^{n-1} \lambda_{jik} p_k(\mathbf{z}) + c_{ij} \right] \cdot C^i \cdot \phi \circ (\phi^{-1} \circ S(\mathbf{z}))^{q^j} \right]$$

$$\phi \circ \mathcal{G} \circ \phi^{-1} \circ S(\mathbf{z}) = \phi \circ \mathcal{H} \circ \phi^{-1} \circ S(\mathbf{z}) - \sum_{j=0}^{r} \sum_{i=0}^{n-1} \sum_{k=0}^{n-1} \lambda_{jik} p_k(\mathbf{z}) \cdot C^i \cdot \phi \circ (\phi^{-1} \circ S(\mathbf{z}))^{q^j} - \sum_{j=0}^{r} \sum_{i=0}^{n-1} c_{ij} \cdot C^i \cdot \phi \circ (\phi^{-1} \circ S(\mathbf{z}))^{q^j}.$$

Sean M_ϕ^j y S las matrices asociadas a las transformaciones lineales $\phi \circ (\phi^{-1}(\mathbf{z}))^{q^j}$ y $S(\mathbf{z})$ respectivamente, entonces

$$\phi \circ (\phi^{-1} \circ S(\mathbf{z}))^{q^j} = M_\phi^i \cdot S \cdot \mathbf{z}\,.$$

Denotemos por

$$B^{(k)} = \begin{bmatrix} b_{11}^{(k)} & \dots & b_{1n}^{(k)} \\ \vdots & \dots & \vdots \\ b_{n1}^{(k)} & \dots & b_{nn}^{(k)} \end{bmatrix},$$

la matriz resultante de

$$\sum_{j=0}^{r} \sum_{i=0}^{n-1} \lambda_{jik} \cdot C^i \cdot M_\phi^i \cdot S$$

y sea $\mathbf{v} = \sum_{j=0}^{r} \sum_{i=0}^{n-1} c_{ij} \cdot C^i \cdot \phi \circ (\phi^{-1} \circ S(\mathbf{z}))^{q^j}$. Entonces

$$\begin{aligned} \phi \circ \mathcal{G} \circ \phi^{-1} \circ S(\mathbf{z}) &= \phi \circ \mathcal{H} \circ \phi^{-1} \circ S(\mathbf{z}) - \sum_{k=0}^{n-1} p_k(\mathbf{z}) B^{(k)} \cdot \mathbf{z} - \mathbf{v} \\ &= \phi \circ \mathcal{H} \circ \phi^{-1} \circ S(\mathbf{z}) - \left[\sum_{k=0}^{n-1} \sum_{i=0}^{n-1} b_{1(i+1)}^{(k)} p_k(\mathbf{z}) z_i, \dots, \sum_{k=0}^{n-1} \sum_{i=0}^{n-1} b_{n(i+1)}^{(k)} p_k(\mathbf{z}) z_i \right] - \mathbf{v}. \end{aligned}$$

Sea $(g_0(\mathbf{z}), \dots, g_{n-1}(\mathbf{z})) = \phi \circ \mathcal{G} \circ \phi^{-1}(\mathbf{z})$, el proceso anterior implica que

$$\begin{aligned} (g_0(S(\mathbf{z})), \cdots, g_{n-1}(S(\mathbf{z}))) &= T^{-1}(q_0(\mathbf{z}), \cdots, q_{n-1}(\mathbf{z})) \\ &\quad - \left[\sum_{k=0}^{n-1} \sum_{i=0}^{n-1} b_{1(i+1)}^{(k)} p_k(\mathbf{z}) z_i, \dots, \sum_{k=0}^{n-1} \sum_{i=0}^{n-1} b_{n(i+1)}^{(k)} p_k(\mathbf{z}) z_i \right] - \mathbf{v}, \quad (3.2) \end{aligned}$$

donde $(q_0(\mathbf{z}), \cdots, q_{n-1}(\mathbf{z})) = T \circ \phi \circ \mathcal{H} \circ \phi^{-1} \circ S(\mathbf{z})$ es la segunda parte de la llave pública de HiRaC.

Sabemos que la matriz M asociada a la parte cubica o cuadrática del polinomio $\mathcal{G} \in \mathbb{K}[X]$ posee rango bajo r^2, por tanto

$$\mathsf{rank}\left(\sum_{i=0}^{n-1} y^i G_i\right) \leq r^2,$$

donde G_l es la matriz asociada a la parte cúbica o cuadrática del $l-$ésimo polinomio en la tupla $\phi \circ \mathcal{G} \circ \phi^{-1}$.

De la ecuación (3.2) tenemos que la componente $l-$ésima de $\phi \circ \mathcal{G} \circ \phi^{-1}$ tiene la forma

$$g_l(z) = \sum_{i=0}^{n-1} t_i^{(l)} q_i(\mathbf{z}) - \sum_{k=0}^{n-1}\sum_{i=0}^{n-1} b_{li}^{(k)} \cdot p_k(\mathbf{z}) z_i - \mathbf{v}[l], \tag{3.3}$$

donde las $t_i^{(l)}$ son las componentes de la transformación lineal $T^{-1}(\mathbf{z})$.

Notemos que los polinomios $p_k(\mathbf{z})$ son cuadráticos, lo que implica que los polinomios $p_k(\mathbf{z})z_i$ son cúbicos. Denotemos por P_{ki} y Q_i las matrices asociadas a la parte cuadrática o cúbica de los polinomios cúbicos $p_k(\mathbf{z})z_i$ y $q_i(\mathbf{z})$ respectivamente. Entonces de la ecuación (3.3) obtenemos la igualdad

$$G_l = \sum_{i=0}^{n-1} t_i^{(l)} Q_i - \sum_{k=0}^{n-1}\sum_{i=0}^{n-1} b_{li}^{(k)} P_{ki}. \tag{3.4}$$

Dado que $\mathsf{rank}(M) \leq r^2$ entonces

$$\mathsf{rank}\left(\sum_{l=0}^{n-1} y^l \left[\sum_{i=0}^{n-1} t_i^{(l)} Q_i - \sum_{k=0}^{n-1}\sum_{i=0}^{n-1} b_{li}^{(k)} P_{ki}\right]\right) = \mathsf{rank}\left(\sum_{i=0}^{n-1} \psi_i Q_i - \sum_{k=0}^{n-1}\sum_{i=0}^{n-1} \Phi_{ik} P_{ki}\right) \leq r^2 \tag{3.5}$$

donde los ψ_i son combinaciones de los $t_i^{(l)}$ y y^l, mientras que los Φ_{ik} son combinaciones de los s_w, y^l y λ_{ijk}.

3.2. Ataque de rango mínimo cuadrático

Nuestro objetivo en esta sección es mostrar que no podemos atacar HiRaC a partir de las matrices que representan la parte cuadrática de los polinomios de la llave pública. Dado que en (3.5) tenemos n^2 matrices P_{ki} que con alta probabilidad son linealmente independientes y por tanto las soluciones del problema de rango mínimo serán triviales.

Supongamos que las matrices Q_i y P_{ki} están asociadas a la parte cuadrática de los polinomios de la llave pública de HiRaC. El espacio de las matrices cuadradas simétricas tiene una dimensión de $\frac{n(n+1)}{2}$. Además, en (3.5) tenemos una combinación lineal de $n+n^2$ matrices, específicamente tenemos n^2 matrices P_{ki} provenientes de los polinomios $p_k(\mathbf{z})z_i$. Entonces como n^2 es mayor asintóticamente que $\frac{n(n+1)}{2}$, a continuación veremos que con alta probabilidad las matrices P_{ki} son una base de las matrices simétricas.

Nuestro objetivo a continuación es ver que con alta probabilidad el conjunto de las partes cuadráticas de los polinomios $p_k(z)z_i$ es una base de todos los polinomios homogéneos cuadráticos y por tanto las matrices P_{ik} son una base de las matrices simétricas cuadradas.

Consideremos el conjunto $A_i = \{z_i z_j : 0 \leq j \leq n-1\}$ y notemos que

$$\text{span}\,(A_0 \cup \cdots \cup A_{n-1}) = \text{El conjunto de todos los polinomios cuadráticos.}$$

Denotemos por $p_k^{(l)}$ la parte lineal de los polinomios cuadráticos p_k. Asumimos que los polinomios p_k son escogidos aleatoriamente por tanto los polinomios $p_k^{(l)}$ son aleatorios sobre el conjunto de los polinomios lineales. Entonces, para i fijo, el conjunto de polinomios $B_i = \{p_k^{(l)}(z)z_i : 0 \leq k \leq n-1\}$ es escogido uniformemente sobre $\text{span}(A_i)$. Más aún, con una probabilidad de

$$\prod_{i=1}^{n}\left(1 - \frac{1}{q^n}\right)$$

B_i es una base de $\text{span}(A_i)$.

El siguiente lema nos permite afirmar que con alta probabilidad el conjunto

$$B_0 \cup \cdots \cup B_{n-1} = \{p_k^l(z)z_i : 0 \leq k, i \leq n-1\}$$

es una base para el conjunto de todos los polinomios cuadráticos homogéneos.

Lema 3.2.1. *Sean $A_1, \ldots, A_n$ y $B_1, \ldots, B_n$ tales que $\text{span}(B_i) = \text{span}(A_i)$ para cada $i = 1, \ldots, n$. Entonces*

$$\text{span}(B_1 \cup \cdots \cup B_n) = \text{span}(A_1 \cup \cdots \cup A_n).$$

Demostración. Para cada $i = 1, \ldots, n$ se tiene que $A_i \subseteq \text{span}(B_i)$, por tanto

$$A_1 \cup \cdots \cup A_n \subseteq \text{span}(B_i) \cup \cdots \cup \text{span}(B_n).$$

entonces

$$\text{span}(A_1 \cup \cdots \cup A_n) \subseteq \text{span}(B_1 \cup \cdots \cup B_n).$$

Notemos que $B_i \subseteq \text{span}(A_i)$ para cada $i = 1, \ldots, n$, de donde

$$B_1 \cup \cdots \cup B_n \subseteq \text{span}(A_1) \cup \cdots \cup \text{span}(A_n) \subseteq \text{span}(A_1 \cup \cdots \cup A_n)$$

concluimos que

$$\text{span}(B_1 \cup \cdots \cup B_n) \subseteq \text{span}(A_1 \cup \cdots \cup A_n).$$

□

Dada una matriz $\mathcal{G}$ de rango bajo r^2, se espera que la solución de la inecuación (3.5) está únicamente determinada por la matriz. Sin embargo dado que con alta probabilidad las matrices P_{ki} son una base de las matrices simétricas cuadradas, podemos obtener una combinación lineal que nos permita construir cualquier matriz de rango r^2. Es decir, no hay manera de garantizar que la solución de (3.5) esté relacionada con la matriz $\mathcal{G}$ y por tanto el ataque de rango mínimo no ofrece información de la llave privada de HiRaC.

3.3. Ataque de rango mínimo cúbico por diferenciales

Dado que un ataque de rango mínimo cuadrático para HiRaC basado en la parte cuadrática de los polinomios de la llave pública nos brinda soluciones triviales, debemos enfocar el ataque en su parte cúbica. Una manera de realizar esto es hallar los diferenciales de los polinomios cúbicos de la llave pública y trabajar con las matrices cuadráticas asociadas a estos diferenciales. Una vez obtenidas estas matrices podemos reducir el problema de rango mínimo cúbico para HiRaC a un problema de rango mínimo cuadrático.

Para esto último supongamos que las matrices Q_i y P_{ki} están asociadas a la parte cúbica homogénea de los polinomios $Q_i(\mathbf{z})$ y $p_k(\mathbf{z})z_i$ respectivamente.

Sea $f(\mathbf{x})$ un polinomio cúbico y consideremos sus diferenciales definidos como

$$D_{\mathbf{a}}f(\mathbf{x}) := f(\mathbf{x}+\mathbf{a}) - f(\mathbf{x}) - f(\mathbf{a}).$$

En [EO$^+$] se muestra que el rango de una combinación de los diferenciales en $\mathbf{a} = \mathbf{e}_k$ está acotado por el rango de la matriz cúbica A asociada a $f(\mathbf{x})$. Más aún si el rango de A es r, con $r \ll n$, entonces el rango de la combinación de los diferenciales es muy cercano a r. Además, es posible asociar cada diferencial con una tajada de la matriz A y por tanto expresar el ataque de rango mínimo cúbico por diferenciales de la siguiente manera. Dada una matriz A con rango $r \ll n$ entonces existe una combinación lineal de las tajadas de A con rango cercano a r.

En el caso de HiRaC tenemos que existe una combinación lineal de las tajadas de Q_i y P_{ki} con rango menor o igual a r^2. Ahora sin pérdida de generalidad podemos asumir que los polinomios cúbicos $p_z(\mathbf{z})z_i$ son aleatorios y por ende las matrices P_{ki} pueden ser consideradas aleatorias. Entonces cada tajada puede ser considerado como una matriz cuadrada aleatoria. Tenemos en total $n(n+n^2)$ tajadas provenientes de las matrices P_{ki}, a partir de un razonamiento similar al utilizado en la sección anterior, podemos concluir que existe un conjunto de tajadas que con alta probabilidad es una base para todas las matrices cuadradas simétricas. Esto implica que cualquier ataque de rango mínimo cuadrático planteado a partir de las tajadas nos llevaría a soluciones triviales.

3.4. Ataque de rango mínimo cúbico

Cualquier aproximación por matrices cuadráticas para resolver el problema de rango mínimo para HiRaC es inviable, por ende, debemos analizar la complejidad de resolver este problema utilizando directamente la definición de rango cúbico. Para esto primero mostraremos cómo reducir el problema de rango mínimo cúbico en un sistema KS y a partir de esto hacer un estimado de su complejidad.

Sea $A \in \mathbb{F}^{n\times n\times n}$, de [EO$^+$] sabemos que A tiene rango r si y sólo si existen r matrices de rango uno $S_1, \ldots, S_r$ tales que

$$\operatorname{span}(A[1,\cdot,\cdot], \ldots, A[n,\cdot,\cdot]) = \operatorname{span}(S_1, \ldots, S_r).$$

Más aún, si $r \ll n$ las primeras r tajadas de A son linealmente independientes y por tanto

$$\operatorname{span}(A[1,\cdot,\cdot], \ldots, A[r,\cdot,\cdot]) = \operatorname{span}(S_1, \ldots, S_r). \tag{3.6}$$

Sea $A^{(i)} = A[i,.,.]$ para $i = 1, \ldots, n$, las n tajadas de A. De acuerdo a la ecuación (3.6) podemos plantear las $n - r$ ecuaciones

$$\sum_{j=1}^{r} \alpha_{lj} A^{(j)} - A^{(l+r)} = 0 \qquad l = 1, \cdots, n-r. \tag{3.7}$$

Cada ecuación del sistema anterior genera las n^2 ecuaciones de la forma

$$\sum_{k=1}^{r} \alpha_{lk} a_{ij}^{(k)} - a_{ij}^{(l+r)} = 0,$$

donde $a_{ij}^{(k)}$ es la componente (i,j) de $A^{(k)}$. Si tomamos las ecuaciones presentes en la primera columna de cada una de las $(n-r)$ matrices resultantes del sistema (3.7) podemos plantear la ecuación

$$\begin{bmatrix} -a_{11}^{(r+1)} & \ldots & -a_{11}^{(n)} & a_{11}^{(1)} & \ldots & a_{11}^{(r)} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ -a_{n1}^{(r+1)} & \ldots & -a_{n1}^{(n)} & a_{n1}^{(1)} & \ldots & a_{n1}^{(r)} \end{bmatrix} \begin{bmatrix} I_{n-r} \\ K^{\intercal} \end{bmatrix} = 0,$$

la cual es exactamente la ecuación

$$\begin{bmatrix} -A^{(r+1)}[\cdot,1] & \ldots & -A^{(n)}[\cdot,1] & A^{(1)}[\cdot,1] & \ldots & A^{(r)}[\cdot,1] \end{bmatrix} \begin{bmatrix} I_{n-r} \\ K^{\intercal} \end{bmatrix} = 0,$$

donde

$$K = \begin{bmatrix} \alpha_{11} & \ldots & \alpha_{1r} \\ \vdots & \ddots & \vdots \\ \alpha_{(n-r)1} & \ldots & \alpha_{(n-r)r} \end{bmatrix}.$$

Esto permite expresar la ecuación (3.7) de la siguiente manera. Consideremos cada matriz A^i como un vector columna

$$A^{(i)} = (a_{11}^{(i)}, \ldots, a_{n1}^{(i)}, a_{12}^{(i)}, \ldots, a_{n2}^{(i)}, \ldots, a_{n1}^{(i)}, \ldots, a_{nn}^{(i)})^{\intercal},$$

entonces el sistema (3.7) es equivalente al sistema de ecuaciones

$$\begin{bmatrix} -A^{(r+1)} & \ldots & -A^{(n)} & A^{(1)} & \ldots & A^{(r)} \end{bmatrix} \begin{bmatrix} I_{n-r} \\ K^{\intercal} \end{bmatrix} = 0. \tag{3.8}$$

Consideremos ahora un problema de rango mínimo con n matrices cúbicas $A_1, \cdots, A_n \in \mathbb{F}^{n \times n \times n}$ con rango objetivo r. Entonces queremos encontrar $\lambda_1, \ldots, \lambda_n$ tales que

$$\mathsf{rank}\left(\sum_{i=1}^{n} \lambda_i A_i\right) \leq r, \tag{3.9}$$

de acuerdo a (3.8) resolver este problema de rango mínimo cúbico es equivalente a resolver el sistema KS

$$\left(\sum_{i=1}^{n} \lambda_i M_i\right) \begin{bmatrix} I_{n-r} \\ K^\intercal \end{bmatrix} = 0, \tag{3.10}$$

donde

$$M_i = \begin{bmatrix} -A_i^{(r+1)} & \cdots & -A_i^{(n)} & A_i^{(1)} & \cdots & A_i^{(r)} \end{bmatrix}.$$

En el caso de HiRaC, el problema de rango mínimo puede ser solucionado resolviendo un sistema KS $\mathcal{F} = 0$, donde $\mathcal{F} \in KS(n^2 \times n, n^2 + n, r^2)$, dado por

$$\left(\sum_{i=0}^{n-1} \psi_i B_i - \sum_{i=0}^{n-1}\sum_{k=0}^{n-1} \psi_{ik} B_{ik}\right) \begin{bmatrix} I_{n-r^2} \\ K^\intercal \end{bmatrix} = 0 \tag{3.11}$$

donde

$$B_i = \begin{bmatrix} -Q_i^{(r^2+1)} & \ldots & -Q_i^{(n)} & Q_i^{(1)} & \ldots & Q_i^{(r^2)} \end{bmatrix}$$

y

$$B_{ik} = \begin{bmatrix} -P_{ik}^{(r^2+1)} & \ldots & -P_{ik}^{(n)} & P_{ik}^{(1)} & \ldots & P_{ik}^{(r^2)} \end{bmatrix},$$

son elementos de $\mathbb{F}^{n^2 \times n}$. A partir de [VBC+19] podemos establecer que cota de la complejidad de resolver este problema está dada por

$$O\left(\left(\begin{array}{c} r^2 k + d_{ks} + 1 \\ d_{ks} + 2 \end{array}\right)^w\right),$$

donde $d_{ks} = \lceil \frac{n(r^2-1)+r^2}{2n+1} \rceil$ y k representa el número de vectores del kernel.

3.5. Ataque a la encripción de HiRaC a partir del ataque de rango mínimo.

En esta sección mostraremos cómo utilizar las soluciones del ataque de rango mínimo para poder desencriptar un mensaje cifrado con HiRaC. A diferencia de otros criptosistemas MPKC, donde podemos construir llaves equivalentes, en HiRaC podemos atacar directamente la inscripción a partir de la información hallada.

Sean los vectores $\boldsymbol{\psi} = (\psi_1, \ldots, \psi_n)$ y $\boldsymbol{\Phi}_k = (\Phi_{k1}, \ldots, \Phi_{kn})$ con $k = 1, \ldots, n$, las soluciones del problema de rango mínimo (3.5). Entonces podemos construir un polinomio $\mathcal{G}^*(X) \in \mathbb{K}$ asociado a la matriz

$$\sum_{i=0}^{n-1} \psi_i Q_i - \sum_{k=0}^{n-1}\sum_{i=0}^{n-1} \Phi_{ik} P_{ki}.$$

El ataque de rango mínimo nos garantiza que el polinomio $\mathcal{G}^*(X)$ posee rango bajo. Aunque en principio $\mathcal{G}^*$ podría ser diferente a $\mathcal{G}$, en los experimentos realizados se observó que se encuentra una sola solución al problema de rango mínimo que corresponde exactamente a $\mathcal{G}$.

A partir de (3.5) tenemos que

$$(T^{-1})^{\intercal}(\mathbf{y}) = \boldsymbol{\psi},$$

donde $\mathbf{y} = (y^0, \ldots, y^{n-1})^{\intercal}$. Más aun,

$$\begin{bmatrix} t_{11} & \ldots & t_{1n} \\ \vdots & \ddots & \vdots \\ t_{n1} & \ldots & t_{nn} \end{bmatrix} \begin{pmatrix} y^0 \\ \vdots \\ y^{n-1} \end{pmatrix} = \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_n \end{pmatrix}, \tag{3.12}$$

entonces podemos concluir que la $i-$ésima fila de la transformación lineal $(T^{-1})^{\intercal}$ está dada por $\phi(\psi_i)$. Esto nos permite obtener una transformación T^*, pero no podemos garantizar que esta sea invertible. Sin embargo, si escogemos vectores aleatorios sobre $\mathbb{F}^n$, con alta probabilidad obtenemos una transformación invertible.

Una vez hemos hallado T, podemos encontrar la función $\mathcal{H} \circ S(X)$. Tomando una transformación lineal S^* aleatoria podemos hallar una función $\mathcal{H}^*(X)$ que tiene la forma

$$\mathcal{H}^*(X) = \sum_{j=1}^{r} \mathcal{M}_j^*(\mathcal{F} \circ \phi^{-1} \circ S^*(X)) + \mathcal{G}^*(X). \tag{3.13}$$

Por tanto esta función $\mathcal{H}^*(X)$ nos da la misma encripción y desencripción que la función $\mathcal{H}(X)$ de la instancia original de HiRaC. Ahora, dado que conocemos la función $\mathcal{G}^*(X)$ sabemos que la función $\mathcal{J}(X) = \mathcal{H}^*(X) - \mathcal{G}^*(X)$ tiene la forma

$$\mathcal{J}(X) = \sum_{j=1}^{r} \mathcal{M}_j^*(\mathcal{F} \circ \phi^{-1} \circ S^*(X)), \tag{3.14}$$

es decir, $\mathcal{J}(X)$ es una instancia de HiRaC sin ruido. Del teorema 2.5.1, vemos que es posible atacar directamente una instancia de HiRaC sin ruido, por tanto podemos atacar directamente $\mathcal{J}(X)$. En conclusión, dada una instancia de HiRaC podemos realizar un ataque de rango mínimo que nos permite reducir dicha instancia a una sin ruido. Esta instancia sin ruido puede ser atacada eficientemente de manera directa para desencriptar cualquier mensaje cifrado.

Capítulo 4

Resultados

4.1. Resultados experimentales

En este capítulo presentaremos algunos resultados experimentales basados en los resultados obtenidos en el capítulo anterior. Todos los experimentos fueron realizados usando el software Magma V2.23-11 y el código disponible en https://github.com/snayder1992/Minrank-cubico. Los experimentos fueron realizados en un servidor[1] con procesador Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz, ejecutando Linux Red Hat 4.8.5-36.

Como comprobamos en la sección 3.4, resolver un problema de rango mínimo cúbico es equivalente a resolver un sistema KS. En particular, para resolver un problema de rango mínimo cúbico de m matrices en $\mathbb{F}^{n\times n\times n}$ con rango objetivo r, podemos resolver un sistema KS $\mathcal{F} \in KS(n^2 \times n, m, r)$.

En esta sección estudiamos experimentalmente la complejidad de resolver un ataque de rango mínimo cúbico para HiRaC. Para esto realizamos experimentos que nos indiquen el tiempo y memoria utilizada para resolver un sistema de Kipnis y Shamir $KS(n^2 \times n, n^2 + n, r^2)$. Al momento de realizar estos experimentos debemos tener en cuenta varias condiciones a la hora de escoger los parámetros.

La dimensión del espacio de matrices cúbicas simétricas está dado por

$$\sum_{i=0}^{n-1} \frac{(n-i)(n-i+1)}{2},$$

por ende debemos escoger el parámetro n de tal manera que el número de matrices presentes en una instancia del ataque mínimo de HiRaC no alcance o exceda esta dimensión. En caso de que el número de matrices $n + n^2$ sea mayor o igual a la dimensión del espacio de las matrices cúbicas simétricas, con un argumento similar al presentado en la sección 3.2, podemos asegurar que el ataque de rango mínimo para HiRaC no nos daría información de la llave privada del criptosistema.

Otra condición a tener en cuenta es el número de ecuaciones e incógnitas en el sistema KS resultante del ataque de rango mínimo para HiRaC. En (3.11) tenemos $n^2(n - r^2)$

[1]Servidor Gauss financiado por el Proyecto Plan 150x150 Fomento de la cultura de evaluación continua a través del apoyo a planes de mejoramiento de los programas curriculares.

ecuaciones con $n^2 + n + r^2(n - r^2)$ incógnitas, entonces debemos escoger n y r de tal manera que podamos garantizar que este sistema sea sobre determinado.

El grado de regularidad teórico está dado por $D_{ks} = d_{ks} + 2$, este nos permite establecer el momento en que el algoritmo $F4$ está próximo a hallar una solución para el sistema KS. Dada la capacidad de cómputo disponible para realizar los experimentos, debemos trabajar con parámetros que nos garanticen un valor de d_{ks} igual a 3, 4 o 5.

Nuestro objetivo ahora es comparar los datos obtenidos con una instancia real de un problema de rango mínimo cúbico para HiRaC con un problema de rango mínimo que consideramos aleatorio. En la tabla 4.1 mostramos datos al realizar el siguiente experimento: Tomamos una matriz $A \in \mathbb{K}^{n\times n\times n}$ con rango r^2, $m-1$ matrices aleatorias Q_i y coeficientes aleatorios $(a_1, \ldots, a_{m-1}) \in \mathbb{K}^n$. Construimos la matriz

$$Q_m = A - \sum_{i=1}^{m-1} a_i Q_i.$$

Luego hallamos la tupla $(a_1, \ldots, a_{m-1})$ mediante un ataque de rango mínimo cúbico.

q	r	n	m	D_{slv}	tiempo(seg)	MB
5	1	5	30	3	3.78	32.1
5	1	6	42	3	7.46	32
5	1	7	56	3	56.63	96
5	1	8	72	3	391.84	416
11	1	5	30	3	51.8	96
13	1	5	30	3	130.27	192

Tabla 4.1: Minrank cúbico con $m = n^2 + n$, mostramos el tiempo y la memoria utilizada para resolver un problema de rango mínimo cúbico "aleatorio". D_{slv} representa el grado de regularidad experimental en que $F4$ resuelve el problema.

q	r	n	m	D_{slv}	tiempo(seg)	MB
5	1	5	30	3	3.3	32
5	1	6	42	3	1.63	64
5	1	7	56	3	9.36	64
5	1	8	72	3	44.61	64
11	1	5	30	3	3.1	64
13	1	5	30	3	3.31	192

Tabla 4.2: Instancia de minrank cúbico para HiRaC. D_{slv} representa el grado en que $F4$ halla una solución para el ataque de rango mínimo.

En la tabla 4.2 mostramos datos del siguiente experimento: Tomamos el archivo Publickey.mgm para generar una clave pública y privada de HiRaC. Luego realizamos un ataque de rango mínimo basados en la llave pública. Podemos concluir que el ataque de rango mínimo cúbico para HiRaC se comporta similarmente al experimento "aleatorio" presentado en la tabla 4.1. Sin embargo, es de notar que la elección de q afecta el tiempo de ejecución del ataque de rango mínimo cúbico "aleatorio" este parámetro no impacta en el

caso de HiRaC. Además, el grado de regularidad experimental D_{slv} coincide con el grado de regularidad teórico D_{ks}.

4.2. Análisis de complejidad

La complejidad de resolver un ataque de rango mínimo para HiRaC está dada por

$$O\left(\left(\begin{array}{c} r^2k + d_{ks} + 1 \\ d_{ks} + 2 \end{array}\right)^w\right),$$

donde $d_{ks} = \lceil \frac{n(r^2-1)+r^2}{2n+1} \rceil$ y k representa el número de vectores del kernel. k es a lo más $n-r$, por tanto es un parámetro que depende de n. Para r fijo, d_{ks} se comporta asintóticamente como $\frac{r^2+1}{2}$. Esto implica que, para $k = n - r$, la complejidad está acotada por $O(n^{wr^2})$.

Podemos concluir que resolver un problema de rango mínimo para una instancia de HiRaC es polinomial en n, esto implica que con suficiente capacidad de cómputo, es posible romper el esquema criptográfico.

Sin embargo, para la elección correcta de parámetros podemos garantizar cierto nivel de seguridad. En este punto es importante tener en cuenta que el nivel de seguridad está dado por

$$O\left(\log_2\left(\left(\begin{array}{c} r^2k + d_{ks} + 1 \\ d_{ks} + 2 \end{array}\right)^w\right)\right).$$

Entonces, un nivel de seguridad de 128 significa que un atacante tendría que realizar 2^{128} operaciones para llevar a cabo el ataque de rango mínimo.

r	n	d_{ks}	Nivel de seguridad	Tamaño de la llave pública	Grado de $\mathcal{G}(X)$
4	64	3	70 bits	3.21 MB	243
4	128	3	81 bits	51.11 MB	243
4	256	3	91 bits	814.6 MB	243
5	64	5	100 bits	3.21 MB	729
5	128	5	116 bits	51.11 MB	729
5	256	5	131 bits	814.6 MB	729
6	64	6	118 bits	3.21 MB	2187
6	128	6	136 bits	51.11 MB	2187
6	256	6	154 bits	814.6 MB	2187

Tabla 4.3: Niveles de seguridad alcanzado por varios parámetros de HiRaC. El costo computacional para realizar eliminación Gaussiana fue fijado en 2 y el tamaño del campo en $q = 3$. La tabla también muestra el tamaño de la llave publica y el grado D del polinomio $\mathcal{G}(X)$.

La tabla 4.3 muestra los niveles de seguridad alcanzados para varios parámetros de HiRaC. Podemos ver que es posible alcanzar niveles de seguridad superiores a 128 bits. Tomando en cuenta [LV01] y basados en varios estimativos como la progresión de la capacidad de cómputo y otros recursos que afecten el avance del software y hardware disponible, podemos asumir que HiRaC con los parámetros propuestos anteriormente, nos ofrecería una garantía de ser seguro más allá del año 2050.

Para poner en contexto estos resultados, cabe compararlos con criptosistemas vigentes como los de la competición de NIST. Los criptosistemas MPKC que se encuentran seleccionados en el concurso de estandarización de NIST son criptosistemas propuestos para firmas digitales. HiRaC es un criptosistema de encripción, por tanto una comparación directa con los criptosistemas en NIST no es del todo correcta. Sin embargo, dado que estos criptosistemas están basado en la misma idea (son criptosistemas MPKC) podemos comparar algunos valores, como el nivel de seguridad, el tamaño de la llave pública y la eficiencia de la desencripción (firma).

GeMSS [CFMR+17] es uno de los esquemas firma digital que se encuentra en competencia en el concurso de NIST. Con parámetros $n = 177$, $r = 9$ y $q = 2$ GeMSS puede garantizar un nivel de seguridad de 128 Bits y un tamaño de llave pública de 352 KB. HiRaC con parámetros menores puede lograr un nivel de seguridad superior a 128 bits y un tamaño de llave mayor.

Para comparar la eficiencia en encripción de HiRaC con la de firmado de GeMSS, no es justo comparar los tiempos reportados, ya que la implementación de GeMSS es mucho más optimizada. En cambio, podemos comparar el grado de los polinomios centrales de cada sistema, ya que el tiempo de desencripción está dominado por el tiempo para factorizar un polinomio de este grado en el campo grande. En el caso de GeMSS, firmar requiere factorizar un polinomio de grado 513 para lograr un nivel de seguridad de 128 bits. Para HiRaC basta factorizar un polinomio de grado a lo más $D = 3q^r = 243$. Esto nos indica, que con la correcta implementación, encriptar con HiRaC es más eficiente que firmar con GeMSS.

En conclusión, con la elección correcta de parámetros HiRaC es seguro ante un ataque de rango mínimo y su tiempo de encriptación puede ser eficiente. Sin embargo el tamaño de la llave pública puede ser mayor comparado con otros esquemas MPKC. Esto nos invita a encontrar una implementación optimizada antes de proponerlo como un esquema de encripción.

Bibliografía

[BFP11] Luk Bettale, Jean-Charles Faugere, and Ludovic Perret. Cryptanalysis of multivariate and odd-characteristic hfe variants. In *International Workshop on Public Key Cryptography*, pages 441–458. Springer, 2011.

[BFP13] Luk Bettale, Jean-Charles Faugère, and Ludovic Perret. Cryptanalysis of HFE, multi-HFE and variants for odd and even characteristic. *Designs, Codes and Cryptography*, 69(1):1–52, 2013.

[BSFOS99] Jonathan Buss, Gudmund Skovbjerg Frandsen, and Jeffrey O Shallit. The computational complexity of some problems of linear algebra. *Journal of Computer and System Sciences*, 58:572–596, 06 1999.

[CFMR+17] Antoine Casanova, Jean-Charles Faugere, Gilles Macario-Rat, Jacques Patarin, Ludovic Perret, and Jocelyn Ryckeghem. Gemss: A great multivariate short signature. *Submission to NIST*, 2017.

[CGLM08] Pierre Comon, Gene Golub, Lek-Heng Lim, and Bernard Mourrain. Symmetric tensors and symmetric tensor rank. *SIAM Journal on Matrix Analysis and Applications*, 30(3):1254–1279, jan 2008.

[CSTV17] Daniel Cabarcas, Daniel Smith-Tone, and Javier A Verbel. Key recovery attack for zhfe. In *International Workshop on Post-Quantum Cryptography*, pages 289–308. Springer, 2017.

[DGS06] Jintai Ding, Jason E. Gower, and Dieter Schmidt. *Multivariate Public Key Cryptosystems (Advances in Information Security)*. Springer-Verlag, Berlin, Heidelberg, 2006.

[EO+] Daniel Esteban Escudero Ospina et al. *Cubic multivariate cryptosystems based on big field constructions and their vulnerability to a min-rank attack*. PhD thesis, Universidad Nacional de Colombia-Sede Medellín.

[FLDVP08] Jean-Charles Faugère, Françoise Levy-Dit-Vehel, and Ludovic Perret. Cryptanalysis of minrank. In *Proceedings of the 28th Annual Conference on Cryptology: Advances in Cryptology*, CRYPTO 2008, pages 280–296, Berlin, Heidelberg, 2008. Springer-Verlag.

[GJ02] Michael R Garey and David S Johnson. *Computers and intractability*, volume 29. wh freeman New York, 2002.

[HL13] Christopher J. Hillar and Lek-Heng Lim. Most tensor problems are np-hard. *J. ACM*, 60(6):45:1–45:39, November 2013.

[How78] Thomas D. Howell. Global properties of tensor rank. *Linear Algebra and its Applications*, 22(Supplement C):9 – 23, 1978.

[KL07] Jonathan Katz and Yehuda Lindell. Introduction to modern cryptography (chapman & hall/crc cryptography and network security series). 2007.

[KS99] Aviad Kipnis and Adi Shamir. Cryptanalysis of the hfe public key cryptosystem by relinearization. In *Annual International Cryptology Conference*, pages 19–30. Springer, 1999.

[LN97] Rudolf. Lidl and Harald Niederreiter. *Finite fields / Rudolf Lidl, Harald Niederreiter ; foreword by P.M. Cohn*. Cambridge University Press Cambridge ; New York, 2nd ed. edition, 1997.

[LV01] Arjen K. Lenstra and Eric R. Verheul. Selecting cryptographic key sizes. *J. Cryptol.*, 14(4):255–293, January 2001.

[MI88] Tsutomu Matsumoto and Hideki Imai. Public quadratic polynomial-tuples for efficient signature-verification and message-encryption. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 419–453. Springer, 1988.

[Osp16] Daniel Esteban Escudero Ospina. *Groebner Bases and Applications to the Security of Multivariate Public Key Cryptosystems*. PhD thesis, Universidad Nacional de Colombia, 2016.

[Pat95] Jacques Patarin. Cryptoanalysis of the matsumoto and imai public key scheme of eurocrypt'88. pages 248–261, 1995.

[SgS13] Friedland. Shmuel and Małgorzata Stawiska. Best Approximation on Semi-Algebraic Sets and k-border Rank Approximation of Symmetric Tensors. *arxiv.org/pdf/1311.1561*, November 2013.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, October 1997.

[VBC+19] Javier Verbel, John Baena, Daniel Cabarcas, Ray Perlner, and Daniel Smith. On the complexity of "superdetermined"minrank instances. 06 2019.